An improved watermarking algorithm for Internet applications

Christophe Guyeux, Jacques Bahi

An improved watermarking algorithm for Internet applications

Christophe Guyeux* and Jacques M. Bahi*
*University of Franche-Comté
Computer Science Laboratory LIFC, Besançon, France
Email: {christophe.guyeux, jacques.bahi}@univ-fcomte.fr

***Abstract*—In this document is proposed a data hiding scheme ready for Internet applications. An existing algorithm based on chaotic iterations is improved, to respond to some major Internet security concerns, such as digital rights management, communication over hidden channels, and social search engines. By using Reed Solomon error correcting codes and wavelets domain, we show that this data hiding scheme can be improved to solve issues and requirements raised by these Internet fields.**

***Keywords*-Information hiding; Internet security; Wavelets; Error correcting codes; Social search engines; Digital rights management.**

I. Introduction

Information hiding has recently become a major digital technology, especially with the increasing importance and widespread distribution of digital media through the Internet. It encompasses steganography and digital watermarking. The aim of watermarking is to slightly alter some digital documents, like pictures or movies, for a large panel of reasons, such as: copyright protection, control utilization, data description, integrity checking, or content authentication. Various qualities are required for a watermarking method, depending on the aims to reach: discretion, robustness against attacks, *etc*. Many watermarking schemes have been proposed in recent years, which can be classified into two categories: spatial domain [11] and frequency domain watermarking [6], [7]. In spatial domain watermarking, a great number of bits can be embedded without inducing too clearly visible artifacts, while frequency domain watermarking has been shown to be quite robust against JPEG compression, filtering, noise pollution and so on. More recently, chaotic methods have been proposed to encrypt the watermark, or embed it into the carrier image, to improve security.

Information hiding is now an integral part of Internet technologies. In the field of social search engines, for example, contents like pictures or movies are tagged with descriptive labels by contributors, and search results are determined by these descriptions. These collaborative taggings, used for example in Flickr [2] and Delicious [1] websites, contribute to the development of a Semantic Web, in which every Web page contains machine-readable metadatas that describe its content. Information hiding technologies can be used for embedding these metadatas. The advantage of its use is the possibility to realize social search without websites and databases: descriptions are directly embedded into media, whatever their formats. Robustness is required in this situation, as descriptions should resist to modifications like resizing, compression, and format conversion.

The Internet security field is also concerned by watermarking technologies. Steganography and cryptography are supposed to be used by terrorists to communicate through the Internet. Furthermore, in the areas of defense or in industrial espionage, many information leaks using steganographic techniques have been discovered. Lastly, watermarking is often cited as a possible solution to digital rights managements issues, to counteract piracy of digital work in an Internet based entertainment world[9].

In this paper, the desire is to improve the robustness of the watermarking algorithm proposed in [3], to respond to Internet security concerns recalled above. The robustness of the watermarking algorithm through geometric attacks is improved by using Reed Solomon correcting codes, whereas the capacity to withstand JPEG compression and noise pollution attacks is enlarged by embedding the watermark into the wavelets domain. Due to its improved robustness, this scheme is suitable for tagging multimedia contents in a social web search context. Additionally, the proposed algorithm possesses various properties of chaos and is secure (see [3]), so it is suitable when desiring to establish a hidden communication channel through the Internet, or for digital rights management. Lastly, watermark encryption and authentication are possible, which enlarge the variety of use in Internet security applications.

The rest of this paper is organized as follows. Firstly, some basic definitions concerning chaotic iterations and topological chaos are given in Section II. The data hiding scheme used in this paper is recalled in the same section. In Section III, the way to use Reed Solomon error correcting codes to improve robustness against geometric attacks is given. Then it is explained in Section IV how to improve robustness against frequency domain attacks by using wavelets coefficients into our scheme. The paper ends with a conclusion section where the contribution is summed up and the planned future work is discussed.

II. Basic recalls

This section is devoted to the recall of the data hiding scheme, which will be improved in Sections III and IV. To do so, basic notations and terminologies in the fields of chaotic iterations and topological chaos are introduced.

A. Chaotic iterations and Devaney's chaos

1) Chaotic iterations: In the sequel S^n denotes the n^{th} term of a sequence S, V_i denotes the i^{th} component of a

vector V, and $f^k = f \circ ... \circ f$ is for the k^{th} composition of a function f. Finally, the following notation is used: $[\![1; N]\!] = \{1, 2, \ldots, N\}$.

Let us consider a *system* of a finite number M of *cells*, so that each cell has a boolean *state*. Then a sequence of length M of boolean states of the cells corresponds to a particular *state of the system*. A sequence which elements belong in $[\![1; \mathsf{M}]\!]$ is called a *strategy*. The set of all strategies is denoted by $\mathbb{S}$.

Definition 1 Let $S \in \mathbb{S}$. The *shift* function is defined by $\sigma : (S^n)_{n\in\mathbb{N}} \in \mathbb{S} \longrightarrow (S^{n+1})_{n\in\mathbb{N}} \in \mathbb{S}$ and the *initial function* i is the map which associates to a sequence, its first term: $i : (S^n)_{n\in\mathbb{N}} \in \mathbb{S} \longrightarrow S^0 \in [\![1; \mathsf{M}]\!]$.

Definition 2 The set $\mathbb{B}$ denoting $\{0, 1\}$, let $f : \mathbb{B}^{\mathsf{M}} \longrightarrow \mathbb{B}^{\mathsf{M}}$ be a function and $S \in \mathbb{S}$ be a strategy. Then, the so-called *chaotic iterations* are defined [10] by $x^0 \in \mathbb{B}^{\mathsf{M}}$ and $\forall n \in \mathbb{N}^*$, $\forall i \in [\![1; \mathsf{M}]\!]$,

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i, \\ \left(f(x^{n-1})\right)_{S^n} & \text{if } S^n = i. \end{cases} \quad (1)$$

In other words, at the n^{th} iteration, only the S^n-th cell is "iterated".

2) Devaney's chaotic dynamical systems: Consider a metric space $(\mathcal{X}, d)$ and a continuous function $f : \mathcal{X} \longrightarrow \mathcal{X}$. f is said to be *topologically transitive* if, for any pair of open sets $U, V \subset \mathcal{X}$, there exists $k > 0$ such that $f^k(U) \cap V \neq \varnothing$. $(\mathcal{X}, f)$ is said to be *regular* if the set of periodic points is dense in $\mathcal{X}$. f has *sensitive dependence on initial conditions* if there exists $\delta > 0$ such that, for any $x \in \mathcal{X}$ and any neighborhood V of x, there exists $y \in V$ and $n \geqslant 0$ such that $|f^n(x) - f^n(y)| > \delta$. δ is called the *constant of sensitivity* of f.

Quoting Devaney in [8], a function $f : \mathcal{X} \longrightarrow \mathcal{X}$ is said to be "chaotic" on $\mathcal{X}$ if $(\mathcal{X}, f)$ is regular, topologically transitive, and has sensitive dependence on initial conditions. When f is chaotic, then the system $(\mathcal{X}, f)$ is highly unpredictable because of regularity and sensitive dependence on initial conditions. Moreover, it cannot be simplified (broken down or decomposed into two subsystems which do not interact) because of topological transitivity. These chaotic dynamical systems then present behaviors very similar to physical noise sources.

In [4], a rigorous theoretical framework has been introduced for the study of chaotic iterations. It has been proven that chaotic iterations (CIs) presented above satisfy topological chaos properties, which leads to improve the security of data hiding schemes based on CIs.

B. Definition of a chaos-based data hiding algorithm

1) Most and least significant coefficients: Let us define the notions of most and least significant coefficients of an image.

Definition 1 For a given image, most significant coefficients (in short MSCs), are coefficients that allow the description of the relevant part of the image, *i.e.* its richest part (in terms of embedding information), through a sequence of bits.

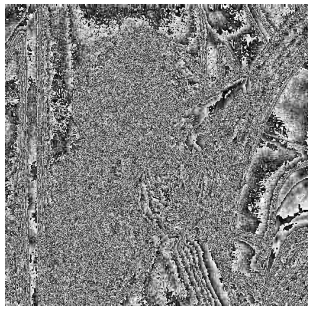
For example, in a spatial description of a grayscale image, a definition of MSCs can be the sequence constituted by the first four bits of each pixel (see Figure 1). In a discrete cosine frequency domain description, each 8×8 block of the carrier image is mapped onto a list of 64 coefficients. The energy of the image is mostly contained in a determined part of themselves, which can constitute a possible sequence of MSCs.

Definition 2 By least significant coefficients (LSCs), we mean a translation of some insignificant parts of a medium in a sequence of bits (insignificant can be understand as: "which can be altered without sensitive damages").

These LSCs can be, for example, the last three bits of the gray level of each pixel (see Figure 1). Discrete cosine, Fourier, and wavelet transforms can be used also to generate LSCs and MSCs. Moreover, these definitions can be extended to other types of media.

(a) Lena.

(b) MSCs of Lena.



(c) LSCs of Lena ($\times$17).

Figure 1. Example of most and least significant coefficients of Lena.

LSCs are used during the embedding stage. Indeed, some of the least significant coefficients of the carrier image will be chaotically chosen and switched, or replaced by the bits of the watermark. The MSCs are only useful in case of authentication; mixture and embedding stages depend on them. Hence, a coefficient should not be defined at the same time as a MSC and a LSC: the last can be altered while the first is needed to extract the watermark.

2) Stages of the algorithm: Our data hiding scheme consists of two stages: (1) mixture of the watermark and (2) its embedding.

Watermark mixture: Firstly, for safety reasons, the watermark can be mixed before its embedding into the image. A common way to achieve this stage is to use the bitwise exclusive or (XOR), for example between the watermark and a pseudo-random binary sequence provided

by the generator defined in [5]. In this paper, we introduce a new mixture scheme based on chaotic iterations. Its chaotic strategy will be highly sensitive to the MSCs, in the case of an authenticated watermarking.

Watermark embedding: Some LSCs will be switched, or substituted by the bits of the possibly mixed watermark. To choose the sequence of LSCs to be altered, a number of integers, less than or equal to the number M of LSCs corresponding to a chaotic sequence U, is generated from the chaotic strategy used in the mixture stage. Thus, the U^k-th least significant coefficient of the carrier image is either switched, or substituted by the k^{th} bit of the possibly mixed watermark. In case of authentication, such a procedure leads to a choice of the LSCs which are highly dependent on the MSCs [4].

On the one hand, when the switch is chosen, the watermarked image is obtained from the original image whose LSBs $L = \mathbb{B}^{\mathsf{M}}$ are replaced by the result of some chaotic iterations. Here, the iterate function is the vectorial boolean negation,

$$f_0 : (x_1, ..., x_{\mathsf{M}}) \in \mathbb{B}^{\mathsf{M}} \longmapsto (\overline{x_1}, ..., \overline{x_{\mathsf{M}}}) \in \mathbb{B}^{\mathsf{M}}, \qquad (2)$$

the initial state is L, and the strategy is equal to U. In this case, the whole embedding stage satisfies topological chaos properties (see [4]), but the original medium is needed to extract the watermark. On the other hand, when the selected LSCs are substituted by the watermark, its extraction can be done without the original cover (blind watermarking). In this case, the selection of LSBs still remains chaotic because of the use of a chaotic map, but the whole process does not satisfy topological chaos [4]. The use of chaotic iterations is reduced to the mixture of the watermark. See the following sections for more detail.

Extraction: The chaotic strategy can be regenerated even in the case of an authenticated watermarking, because the MSCs have not been changed during the embedding stage. Thus, the few altered LSCs can be found, the mixed watermark can be rebuilt, and the original watermark can be obtained. In case of a switch, the result of the previous chaotic iterations on the watermarked image should be the original cover. The probability of being watermarked decreases when the number of differences increase.

If the watermarked image is attacked, then the MSCs will change. Consequently, in case of authentication and due to the high sensitivity of the embedding sequence, the LSCs designed to receive the watermark will be completely different. Hence, the result of the recovery will have no similarity with the original watermark.

The chaos-based data hiding algorithm is summed up in Figure 2.

III. Improving robustness against geometric attacks

In this section, we are interested in improving our scheme to make its use relevant in a social web search context. The idea is to embed the tag of a given image into its pixel values. As neither the cover image nor the tag should be required during a search, the LSBs will be

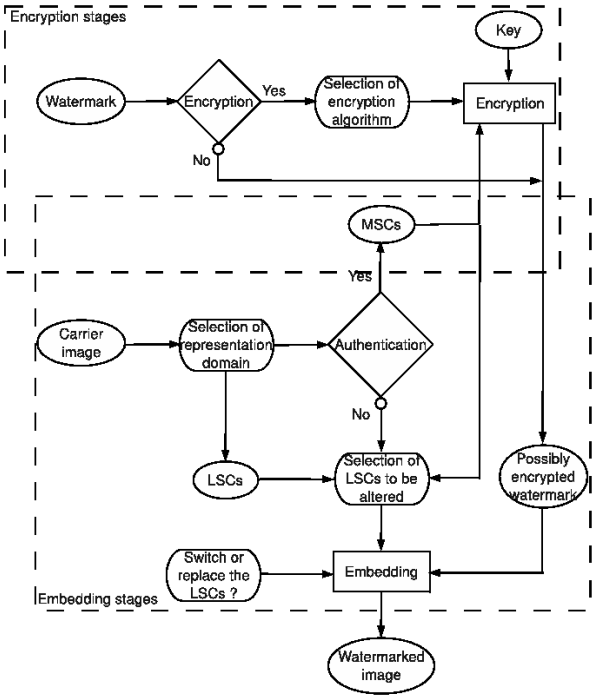


Figure 2. The chaos-based data hiding algorithm.

replaced (not switched), by the tags. Authentication is not required, as man-in-the-middle attacks are not supposed to occur. However tags are vulnerable to involuntary attacks such as rotation or resizing, so we need to improve robustness against geometric attacks. To do so, the embedding domain will be the spatial domain. This choice leads to a large given payload, so a lot of tags can be embedded into the cover image. Additionally, we will use Reed-Solomon error correcting codes, to reinforce the capacity to extract the watermark from a tagged image, even though it has been altered. As an illustrative example, we will show how to embed the description of the well-known Lena into its own image. Let us remark that the same procedure can be applied to create a hidden channel for communicating through a given web page, for example, by inserting messages in the background image of this website. In this situation, it is recommended to add the encryption stage to improve the security of the hidden channel.

In this illustrative example, the following text extracted from Wikipedia's description of Lena will be inserted into its own image:

```
Lena (Soderberg), a standard test image
originally cropped from the November
1972 issue of Playboy magazine.
```

The cover image will be the Figure 1(a), which is a 256×256 grayscale image. The text to embed is converted into 756 binary digits by using the ASCII table: each of the 109 characters are coded with 7 digits, thus obtaining the following bits flow (called a system):
100110011001011101110110000101000000101000101001111011
111100100110010111100101100010110010111100101100111...

20000 binary digits are computed from a logistic map, with parameters $\mu = 3.999999$, $x^0 = 0.65$, and those binary digits are grouped ten by ten ($10 = \lceil \log_2(756) \rceil$) to obtain an integer sequence S lesser than or equal to 756. So, chaotic iterations are applied to the above system, with chaotic strategy S and the vectorial boolean negation, to obtain the following encrypted message:

00100011111000111000110111011111100001101101001100010100101111000011011001101001000111010110110001011010110...

In this example, there is no authentication step, but Reed-Solomon error correction codes are used to increase the robustness. Here, two layers of Reed–Solomon coding, respectively (32,24)-RS and (24,16)-RS codes, are separated by a 3-way convolutional interleaver operation, to obtain a scheme similar to the Cross-Interleaved Reed Solomon Coding (CIRC) of the compact disc. The message to embed is the result of this coding operation: a 2112 binary stream, starting by:

01011010010110000010000100011100001001110011111110100011101111000000101100011010101110110000100110010011110...

These 2112 bits will be embedded into Lena, an image constituted by $256 \times 256 \times 8 = 524288$ bits (8 bits per pixel). To do so, we will consider the two least significant bits of each pixel as LSCs: a few of them will be replaced by the bits of the watermark. To select these bits to replace, the strategy S of the encryption stage is used again, to generate a sequence of triplets $(x^n, y^n, z^n)_{n \in \mathbb{N}}$ in such a way that $x^n, y^n \in [\![0; 255]\!]^{\mathbb{N}}$, and $z^n \in \{1; 2\}^{\mathbb{N}}$. This generation is realized as follows:

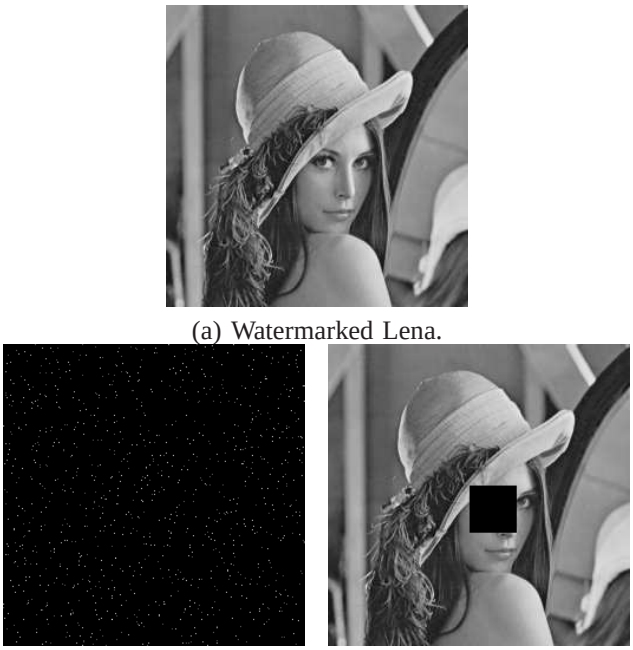
$$\left\{ \begin{array}{lcl} x^0 & = & 11, \\ y^0 & = & 23, \\ z^0 & = & 1, \end{array} \right.$$

and

$$\left\{ \begin{array}{lcll} x^{n+1} & = & 2x^n + S^{3n} + n & (\text{mod } 255), \\ y^{n+1} & = & 2y^n + S^{3n+1} + n & (\text{mod } 255), \\ z^{n+1} & = & 2z^n + S^{3n+2} + n & (\text{mod } 2). \end{array} \right.$$

So the n^{th} bit of the encrypted and encoded binary message is inserted into the z^n least significant bit of the pixel in position (x^n, y^n) of Lena, to obtain the watermarked Lena in Figure 3(a). In Figure 3(b) the differences are shown between the original Lena and the watermarked Lena. This image illustrates the fact that LSCs to be replaced are chaotically chosen and uniformly distributed [4].

In [3], our scheme has been defined without RS codes and its robustness has been evaluated. It is established that the watermark can resist rotation, cropping, JPEG compression, and gaussian noise attacks. However, the extracted watermark is slightly different from the original one and this difference increases with the number of attacks. These errors, which are undesirable in a social web search context, can be corrected by the use of RS codes.



(a) Watermarked Lena.

(b) Differences with Lena. (c) Attacked Lena.

Figure 3. Watermarked Lenas (scale reduced).

To illustrate, the watermarked Lena is zeroed: a square of 40×40 pixels is removed from the image, as in Figure 3(c). So the message is extracted from the watermarked and attacked Lena: the strategy S is regenerated from a logistic map with the same parameters as above. Then the sequences x^n, y^n and z^n can be regenerated too, and the embedded bits can thus be extracted. These bits are decoded in the reverse process: (24,16)-RS decoding, 3-way deinterlacing, and (32,24)-RS decoding codes. Lastly, the resulting bits sequence is decrypted, bits are grouped 7 by 7, and converted into characters with the ASCII table, to obtain the following message:

```
Lena (Soderberg), a standard test image
originally cropped from the November
1972 issue of Playboy magazine.
```

IV. Improving robustness against frequency domain attacks

In this section, the way to use our algorithm in frequency DWT domain is explained. Due to its robustness against frequency attacks such as JPEG compression, this scheme can be used to insert a copyright into a media (digital rights management context).

A. Stages and detail

The carrier image and watermark are the same as in Section III, but Lena is now constituted by 512×512 pixels. The embedding domain is the discrete wavelets domain (DWT). In this paper, the Daubechies family of wavelets is chosen: Lena is converted into its Daubechies-1 DWT coefficients, which are altered by chaotic itera-

tions. The watermark is encrypted by chaotic iterations before its embedding, with the same procedure as above.

Each example below depends on a decomposition level and a coefficient matrix (Figure 4): LL means approximation coefficient, when HH, LH, HL denote respectively diagonal, vertical and horizontal detail coefficients. For example, the DWT coefficient HH2 is the matrix equal to the diagonal detail coefficient of the second level of decomposition of Lena.

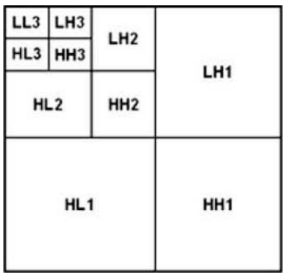


Figure 4. Wavelets coefficients.

To embed the encrypted watermark, LSCs are obtained from the coefficients defined above. The system to iterate is the boolean vector of size 256^2, constituted by these M LSCs of Lena. Iterate function is the vectorial boolean negation, and chaotic strategy U is defined as follows:

$$\begin{cases} U^0 &= S^0 \\ U^{n+1} &= S^{n+1} + 2 \times U^n + n \pmod{\mathsf{M}}. \end{cases} \quad (3)$$

where S denotes the strategy used in the encryption stage (see [3]). Thus, bits of the LSCs are switched, not replaced: the whole embedding process satisfies Devaney's chaos property [4]. However, for this reason, the watermark cannot be extracted: contrary to Section III, we are not in a steganographic framework, but in a pure non-blind watermarking scheme used for digital rights management. To know if a given image I' is the watermarked version of another image I:

- the whole process is applied to I', with the same parameters (LSCs, watermark, *etc.*), to obtain I'',
- I'' is compared to the original I.

To evaluate the differences, the RMS value defined by $\bar{x} = \sqrt{\frac{1}{\mathsf{M}} \sum_{i=1}^{\mathsf{M}} (I - I'')_i^2}$ is computed. The probability that the image has been watermarked increases when the RMS decreases. Indeed, each bit of the LSCs of I'' has been switched an even number of times (the RMS is nonzero because of computational errors).

B. First example: coefficient HH2

1) Embedding: In this first experiment, the watermark is inserted into the diagonal coefficient HH2 (a real matrix of size 128×128). LSCs are the second least significant bit of each integral value of HH2. To do the insertion, chaotic iterations are made. The system to iterate is the boolean vector of size 128^2, constituted by the LSCs of Lena. Iterate function is the vectorial boolean negation and chaotic strategy is defined as in Equation 3, with $U^0 = 1$ and $\mathsf{M} = 256^2$.

(a) Original Lena.

(b) Watermarked Lena.

Figure 5. Data hiding in DWT domain

Table I
RMS VALUES FOR A HH2 EMBEDDING

	HH2 embedding				
	μ	U^0	Iterations	Authentication	RMS
	3.99987	-	-	-	1.131
	-	0.64	-	-	1.129
Encryption	-	-	19950	-	0.796
	-	-	-	MSB = [5,6,7]	1.122
	Coefficient	S^0	LSB	RMS	
	HH1	-	-	253.65	
Embedding	-	2	-	0.653	
	-	-	[1]	0.983	

In this situation, PSNR = 53.45db. Pixel values have been modified by at most of one level of gray. The mean value of differences is equal to 0.294, when RMS = 0.542. The alteration can thus be considered as indistinguishable.

2) Extraction: The system to iterate is constituted by the second least significant bit of each integral value of HH2, the approximation coefficient of the first decomposition level of the watermarked Lena. Iterate function is the vectorial boolean negation and chaotic strategy is computed as above. Thus, the result is compared to the coefficient HH2 of the original Lena. The RMS is equal to 0.129. As a comparison, Table I gives the RMS values resulting on a bad extraction (wrong parameters, *etc.*) Symbol '-' means that the value of the considered parameter is unchanged. We show that the least RMS is obtained for an extraction with the same parameters as the embedding. Let us notice that if the extraction is attempted to the original Lena, RMS is twice greater than 0.127.

C. Second example: coefficient LL1

1) Embedding: In this paragraph, the watermark is inserted into the approximation coefficient LL1 of Lena (a real matrix of size 256×256) and LSCs are the second least significant bit of each integral value of LL1.

To realize the embedding, chaotic iterations are realized as before. The system to iterate is the boolean vector, of size 256^2, constituted by the LSCs of Lena. Iterate function is the vectorial boolean negation, chaotic strategy is defined as in Equation 3 with $U^0 = 1$, and $\mathsf{M} = 256^2$. In this situation, PSNR = 60.06 db. Pixel values have been modified by at most two levels of gray. The mean value of differences is 0.063, when the RMS is equal to 0.245.

Table II
RMS VALUES FOR A LL1 EMBEDDING

	LL1 embedding				
	μ	U^0	Iterations	Authentication	RMS
	3.99987	-	-	-	0.669
	-	0.64	-	-	0.670
Encryption	-	-	19950	-	0.443
	-	-	-	MSB = [5,6,7]	0.667
	Coefficient	S^0	LSB	RMS	
	HH1	-	-	223.737	
Embedding	-	2	-	0.135	
	-	-	[1]	0.548	

For all of these reasons, the alteration can be considered again as indistinguishable.

2) Extraction: The system to iterate is constituted by the second least significant bit of each integral value of LL1. Iterate function is the vectorial boolean negation and chaotic strategy is computed as above. Thus, the result is compared to the coefficient LL1 of the original Lena. In our example, we obtain RMS = 0.127. As a comparison, Table II below gives the RMS values resulting in a bad extraction (wrong parameters, *etc.*) Symbol '-' means that the value of the considered parameter is unchanged. We show that the least RMS is obtained for an extraction with the same parameters as the embedding. Let us remark that if the extraction is tried on the original Lena, then RMS is twice greater than 0.127.

V. DISCUSSION AND FUTURE WORK

In this paper, the robustness of the data hiding scheme proposed in [3] is improved to achieve properties required in Internet applications of data hiding techniques. This scheme depends on a general description of the carrier medium to watermark, in terms of the significance of some coefficients we called MSCs and LSCs. The encryption of the watermark and the selection of coefficients to alter are based on chaotic iterations, which generate topological chaos in the sense of Devaney [4]. Thus, the proposed algorithm has a sufficient level of security for Internet applications, such as digital rights management or social web search.

We have proposed in this paper to enlarge the relevance of our scheme in these contexts by using Reed-Solomon error correcting codes and wavelets domain. The first improvement is relevant in a social web search domain, in which the tags of an image must be recovered exactly, even though the image has faced geometric operations. The use of wavelets domain is linked more to digital rights management. This domain is known to present good results against frequency attacks, which can occur when someone tries to remove some DRM. It can be noticed that these two improvements can be realized together.

Algorithms have been evaluated through attacks and results have been experimentally obtained. Choices that have been made in this first study are simple: spatial and Daubechies domains for the embedding, negation function as iteration function, *etc.* The aim was not to find the best watermarking method generated by our general algorithm, but to explain how to improve robustness for Internet applications.

In future work, other choices of iteration functions and chaotic strategies will be explored and compared in order to increase authentication and robustness to attacks. In addition, new frequency domain representations will be used to select the MSCs and LSCs. Properties induced by topological chaos, such as entropy, will be explored and their role in Internet applications will be explained.

REFERENCES

[1] Delicious social bookmarking, http://delicious.com/.

[2] The frick collection, http://www.frick.org/.

[3] Jacques Bahi and Christophe Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT 2010, International conference on security and cryptography*, pages ***–***, Athens, Greece, 2010. To appear.

[4] Jacques Bahi and Christophe Guyeux. Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10, IEEE World Congress on Computational Intelligence*, pages ***–***, Barcelona, Spain, July 2010. To appear.

[5] Jacques Bahi, Christophe Guyeux, and Qianxue Wang. A novel pseudo-random generator based on discrete chaotic iterations. In *Internet 2009*, pages 71–76, Cannes, France, August 2009.

[6] Jin Cong, Yan Jiang, Zhiguo Qu, and Zhongmei Zhang. A wavelet packets watermarking algorithm based on chaos encryption. *Lecture Notes in Computer Science*, 3980:921–928, 2006.

[7] Zhao Dawei, Chen Guanrong, and Liu Wenbo. A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons and Fractals*, 22:47–54, 2004.

[8] Robert L. Devaney. *An Introduction to Chaotic Dynamical Systems, 2nd Edition*. Westview Pr., March 2003.

[9] Y. Nakashima, R. Tachibana, and N. Babaguchi. Watermarked movie soundtrack finds the position of the camcorder in a theater. *IEEE Transactions on Multimedia*, 2009. Accepted for future publication Multimedia.

[10] F. Robert. *Discrete Iterations: A Metric Study*, volume 6 of *Springer Series in Computational Mathematics*. 1986.

[11] Xianyong Wu, Zhi-Hong Guan, and Zhengping Wu. A chaos based robust spatial domain watermarking algorithm. *Lecture Notes in Computer Science*, 4492:113–119, 2007.